Advanced Security 1 - CMPU4007
Week 2 - Classical Encryption Techniques

In this lab you are required to provide solutions to the questions below.

Caesar cipher

Q 1. Encrypt the following plaintext with the Caesar cipher using key: -3
And I shall remain satisfied, and proud to have been the first who has ever enjoyed the fruit of his writings as fully as he could desire; for my desire has been no other than to deliver over to the detestation of mankind the false and foolish tales of the books of chivalry, which, thanks to that of my true Don Quixote, are even now tottering, and doubtless doomed to fall for ever. Farewell.

Q 2. Decrypt the following ciphertext with the Caesar cipher using an unknown key
Vg jbhyq frrz gung, nf ur rknzvarq gur frireny cbffvovyvgvrf, n fhfcvpvba pebffrq uvf zvaq: gur zrzbel bs ubj ur uvzfrys unq orunirq va rneyvre qnlf znqr uvz nfx jurgure fbzrbar zvtug or uvqvat ure sebz gur jbeyq

Vigenere cipher

Q 3. Encrypt the following plaintext with the Vigenere cipher using key: PASSWORD
I shall (from now on) select and take the ingots individually in my own yard, and I shall exercise against you my right of rejection because you have treated me with contempt.

Q 4. Decrypt the following ciphertext with the Vigenere cipher using an unknown key
Yhwvtroi, 28 Yudq 2016 - Pse bjatw pt foxgf zwjzql bgio qcwelwlar, blsg rmprochek ewrv nsoyr uvs ndcljebv rk pkium hy bef; sjr wutm vljg aybefl ds ydx mchf asx bojw lwfxx, aph fjsbntzaju kkwixit hvbduyzkik wme ylpzs gdrdv. wbu wme mmou olhtsajg wutm mmmzwxv lanebx ejipkt, obn dtzwn avq fnf xicgo lhg sns yxstuqfb oxs fakdsipjn qj uvs uxny zwjv gjskwusr pgoe zqbklsg. cre wt cdmw oafv lstgqqsfkie, lzam ydae eibgsn urge pvvlw ipxfadogafua oj zfs kr uvssg pgoaf; rqi odiewsxi tg ldszu kavlff oxs mgldsi dsd vs uvs oadwjo, we rupqwjhwyc tg lds gdxt cptc wx ihw xqhluj, ba wp oqdxny gj smhwy qgdogsdn, lzam nlql nmws poitwj wbu ptrg lbddsay
Hint: Key length > 10, Known plaintext: Thursday

Deliverables: Please submit the solved plaintexts, ciphertexts, keys,code and notes written.